Journal of Scientific & Industrial Research
Vol. 79, September 2020, pp. 824-828

An Authenticated Enrolment Scheme of Nodes using Blockchain and Prevention of Collaborative Blackhole Attack in WSN

R K Yadav and Rashmi Mishra*

Department of Computer Science and Engineering, Delhi Technological University, New Delhi, India

Received 24 August 2019; revised 28 January 2020; accepted 08 May 2020

Security is indispensable concern part of the WSN. The reliable mechanisms and routing schemes are facing different set of encounters in the era of authentic status quo and it is also very knotty. Problem is identified in the recognition of untrusted nodes and routes followed from source to destination along with the restraint of battery status in WSN. No effective technique is there to avert the vindictive node attack. The current research article provides an algorithm of the nodes by employing the blockchain technology as far as solution to the other persisting drawbacks like identification of untrusted nodes and untrusted routes were tackled out by the help of secure AODV using blockchain. The outcomes of this research article by performing the simulation and experimental validation of the existing systems denotes the successful identification and occurrence of malicious nodes, end-to-end delay, packet delivery ratio and through put performance evaluation. The registration of the nodes in blockchain database and behaviour of black hole attack in AODV protocol was also simulated using NS2 blockchain algorithm.

Keywords: AODV, End-to-end delay, Malicious nodes, Performance evaluation, Untrusted routes

Introduction

The most feasible and available technology used for the transfer of information from one node to another node in an environment is refereed as wireless sensor network (WNS). This information is gathered by employing a larger number of sensor nodes in which the transfer of information can occur in between each other in an environment and simultaneously monitored also.[1] During transmission, sensitive data is transmitted from one node to another therefore security is needed for the data and protection of the network functioning is also required.[2] For the security purpose some of the cryptographic algorithm and blockchain had been used.

Aim and Objectives of the Research

The aim of this research is to authenticate the nodes in WSN by using Blockchain. The proposed algorithm reduces the delay time, increase the packet delivery ratio and also increase the throughput by using Secure-AODV BC protocol. The main objectives of this paper are listed below:

- To improve the packet delivery efficiency rate from source to destination.
- To identify the blackhole node and collaborative blackhole nodes in a network.
- To reduce the bandwidth utilization by the nodes.
- To improve the security of the nodes.

Blockchain Network Procedure

WSN required confidentiality, integrity, authentication, time synchronization, secure localization etc. But having so much security characteristics in WSN, there are some type of attacks such as wormhole, selective forwarding, hello flood, sinkhole, false routing attack, blackhole and collaborative blackhole attacks are there.[3,4] In blackhole attack, there is node which drop the packets coming from the authenticated node and drop the packets. A blackhole attack is easy to find but in collaborative blackhole attack, there are multiple blackhole node is exist which change their behaviour during time to time. So, it is harder to detect the collaborative attack. In view of the above security issues Zheng[5] proposed a solution for the third-party trust management in which author use self-organizing ledger system, blockchain is very suitable for the multi hope distributed wireless sensor network.[6] A lot of research was done by many researchers which carried blockchain in routing algorithm.

*Author for Correspondence
E-mail: dtuphd.rashmi@gmail.com

The blockchain is decentralized database which store all the information on every node authorized by process and mainly deal with security problem and enhanced trust in between the nodes. There are some features of blockchain which differentiate it with other schemes. The first properties are distributed ledger which stores all the information or the transaction in the blockchain such as address of the sender, the amount of money he transfers, nonce, timestamp, hash value of the block etc. The ledger is stored on each node in the network and each node participating in the blockchain have to keep this ledger for the information. This property of the distributed ledger provides the monitoring capability to each and every node so that the legality of the transaction is visible to all the nodes. Second feature of the blockchain is asymmetric encryption and authorization technology. The transaction stored in the blockchain is visible to all but the contents of the entity should be encrypted so that no one is able to access the information without the permission of the data owner or temper the stored information. Third feature if consensus algorithm which provide temper proof environment by using Proof of Work, Proof of Stack, Delegated proof of Stack, Proof of Capacity is discussed by.[5–6] Last feature is smart contract, which provides trusted environment, non-tempering and executed the predefined code stored in the blockchain by blockchain miner. Several researchers have proposed several routing schemes based on the blockchain technology.[7–11]

Experimental Details

Proposed Methodology

In our system, we choose the proof of authority (PoA) consensus algorithm which can progression transaction more capably. PoA will pre-authenticate the nodes in a WSN network. Here PoA will work in different entity such as server node, cluster head.

Registration Process using Blockchain: Registration process of any node is completed by using PoA (Proof of Authority). Assumptions considered for implementation are: RREP header is modified with additional field that is Speed of node, Threshold value of node speed is taken as speed threshold = 100 m/s.

1. Source node create the block, containing encrypted MAC address or physical address//time stamp// nonce//hash value of the block//Pus (Public key of Source) using his private key (PRs) and send it to the server node.

PRs (E, MAC//timestamp//nonce//hash value//PUs)

2. Server node first authenticates the source node then release the blockchain.

If
MAC_Add = ! BC //Address of source (MAC) is not stored in blockchain.
THEN
Server ← MAC_Add //server add the address of source node to the blockchain and generate a token for the node.
Else
Release the blockchain and update the value corresponding to source MAC address to 1.// MAC_Add in BC set to 1.

3. Source node broadcast the generated blockchain to the network.
4. If next node has its MAC address in the block then it passes the block to the next node else add its MAC address to the blockchain, if it's not blackhole node.

Secure AODV Using Blockchain

1. Source S broadcasts RREQ message.
2. IF
{
D replies with RREP
Then
S send the message
}
END IF
3. IF

Node B (intermediate node) replies RREP and packet reaches to the next hope (*) from node A //*preceding node A is in the direction in which RREP is traversing from B towards S.

Then check
{
MAC_address in BC = 1 … (1)
&
(Speed of Node >speed threshold) … (2)
&
(Sequence No> seq_no_threshold) … (3)

// Threshold value is updated every time intermediate node receives a RREQ packet and threshold value of sequence no is calculated as sequence_number_ threshold = sequence number (of RREQ packet) * hop count
If Eqs (1) (2) and (3) are true then
GO TO Step 4.
else
GO TO Step 5.

4. IF (hop count>= 2)

Node X will send a Modified Hello signal with HopCount equal to 2 (in case hopcount = 2)

or

HopCount equal to 3 (in case hopcount > 2) to a Node (*)(*) (say Z) which is few hops (equal to hopcount) away from A.// ** all the values have to be taken from the RREP received from intermediate node B and (*)(*) Z node is in the path through which RREP packet has reached B.

5. IF

A receives acknowledgment from Z successfully then A forwards RREP to S and S will transmit the data.

Else

Node next to B is Blackhole and an alert signal will be transmitted by A to S. Else

Node B is Blackhole node and an alert signal will be transmitted by A to S. Step 5: A forwards RREP to S and S will transmit the data.

Results and Discussion

Implementation and Analysis

Several simulations scenarios on the different approaches are applied. Here represent two different comparison scenarios of the present work. Simulation Parameter used for the implementation are Linux (Ubuntu 12.04, NS-2.35, Number if nodes used for the simulations are 50, 100, 150, 225, 315, Packet size is 512, traffic type is UDP/CBR, Simulation time is 100 sec, antenna type is omni, transmission range is 1000*1000 m and routing protocols used are AODV, Secure-AODV.

The conclusions of the study in this paper are obtainable in three compartments specifically:

Delay Comparison, PDR, Throughput for Single and Cooperative Blackhole Attacks using AODV

The simulation result shows x-axis denotes the simulation node and y-axis shows the performance metrics parameter. Average end-to-end delay is shown in Fig. 1. The average delay of AODV is increased with number of nodes but after a 150-node delay is increased smoothly. The overall performance of average delay for single and cooperative blackhole attack with respect to number of nodes variation are Secure-AODV with hash function verification performance better to AODV protocols. The Performance of packet delivery ratio of single black hole-AODV is increased with 150 nodes. With the variation of number of nodes AODV routing protocol

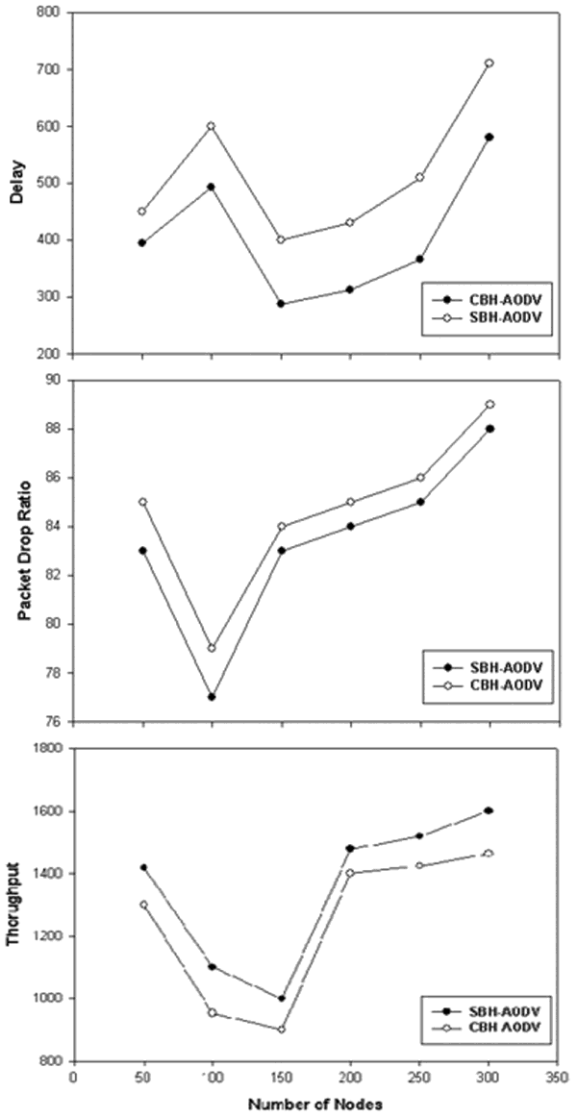

Fig. 1 — End to End Delay, PDR Throughput in AODV

packet delivery ratio is low for the single black hole attack till 150 nodes after 225 nodes it slightly increased as compared to the Cooperative. The performance of throughput for blackhole-AODV for single and cooperative blackhole are almost same for nodes 50, 100, 150 and 225 but throughput after 225 nodes is showing different performance and single blackhole-AODV increase. The maximum delay recorded on comparing both the parameters of CBH and SBH are 35.80 sec and the minimum value recorded so far on the basis of these parameters is 9.30 sec. The maximum PDR recorded on comparing both the parameters of CBH and SBH are 2.53 and the minimum value recorded so far on the basis of these parameters is 1.15. The maximum throughput

recorded on comparing both the parameters of CBH and SBH are 27.27 and the minimum value recorded so far on the basis of these parameters is 6.67.

Single and Cooperative Blackhole Attacks using Secure-AODV using Blockchain

The average end-to-end delay is shown in Fig 2. The average delay of Secure-AODV single blackhole is almost same for node 50, 100 and after 150 nodes its increase and slightly decrease at node 315. The cooperative black holes are showing less delay as compare to single black hole. It's increasing and decreasing with respect to number of node but in AODV-black hole its continuous increasing, so that our proposed Secure-AODV using blockchain is more secure and highly aware to the network. The Performance of packet delivery ratio of single and cooperative black hole in Secure-AODV using blockchain network is continuously increased as compare to AODV- Blackhole; it's increased the packet delivery ratio. The performance of throughput for blackhole-AODV for single and cooperative blackhole almost same for nodes 50, 100, 150 and 225 but as compare to the normal blackhole AODV is better, all results in secure-AODV using blockchain is high. The maximum delay recorded on comparing both the parameters of CBH and SBH is 31.78 sec and the minimum value recorded so far on the basis of these parameters is 5.45 sec. The maximum PDR recorded on comparing both the parameters of CBH and SBH are 3.66 and the minimum value recorded so far on the basis of these parameters are 1.69.The maximum throughput recorded on comparing both the parameters of CBH and SBH are 4.76 and the minimum value recorded so far on the basis of these parameters are zero.

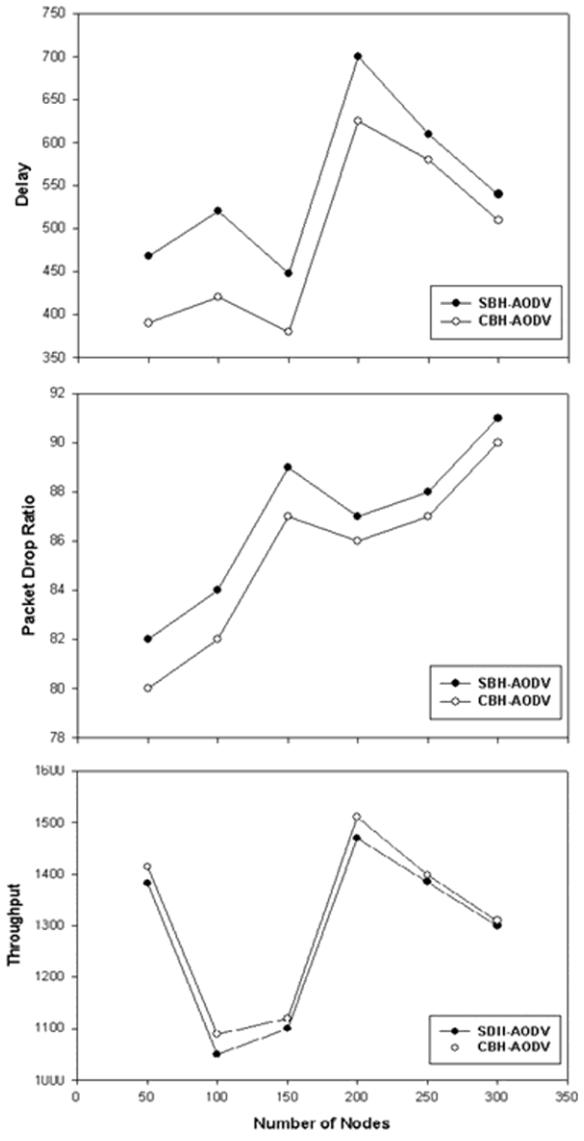

Fig. 2 — End to End Delay, PDR Throughput in secure AODV using blockchain

Conclusions

In this paper, we proposed an authenticated enrolment scheme of nodes using Blockchain and detection and prevention of blackhole and collaborative blackhole attack in WSN. As a decentralized, persistent, distributed ledger, anonymity and auditability in asymmetric encryption and authorization technology blockchain provide a feasible scheme for enrolment process of nodes. So, it is easy to trace the behaviour of each node in a network. By making each node and route perceptible and temper-proof, nodes can acquire dynamic and reliable information on the blockchain network. The detailed AODV and Secure-AODV using blockchain choose the best route and discard the routes having malicious nodes. Finally, experimental and simulation part shows that the result of our system can effectually overwhelm the occurrences of malicious nodes and the end-to-end delay and packet delivery ratio and through performance shows the novelty in research.

References

1 Filippini M, Hunt L C, Energy demand and energy efficiency in the OECD countries, a stochastic demand frontier approach, *Energy J*, **32(2)** (2011) 59–80.

2 Kalkha H, Satori H, & Satori K, A dynamic clustering approach for maximizing scalability in wireless sensor network, *Trans Mach Learn Artif Intel*, **5(4)** August (2017) 637–650.

3 Sarvari S, Sani N F M, Hanapi Z M, Abdullah M T, Wireless local area network, a comprehensive review of attacks and metrics, *J Theor Appl Inf Technol*, 95(13) (2017) 2913–2934.

4 Abraham A, Falcon R, Koeppen M, *Computational Intelligence in Wireless Sensor Networks: Recent Advances and Future Challenges*, Vol. 676, Springer SCI (2017).

5 Angrish A, Craver B, Hasan M, Starly B, A case study for blockchain in manufacturing, a prototype for peer-to-peer network of manufacturing nodes, *Procedia Manuf*, 26 (2018) 1180–1192, arXiv: 1804.01083.

6 Bach L, Mihaljevic B, Zagar M, Comparative analysis of blockchain consensus algorithm, *41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) Opatija*, 2018, pp. 1545–1550, doi: 10.23919/MIPRO.2018.8400278.

7 Lu Z, Sagduyu Y E, Li J H, Securing the backpressure algorithm for wireless networks, *IEEE Trans Mob Computing*, **16** (2017) 1136–1148.

8 Sirisala N, Bindu C S, Recommendations based QoS trusted aggregation and routing in mobile adhoc networks, *Int J Com Network Inf Secur*, **8** (2016) 215.

9 Venkataraman R, Moeller S, Krishnamachari B, Rao T R, Trust-based back pressure routing in wireless sensor networks, *Int J Sens Netw*, **17** (2015) 27–39.

10 Li J, Liang G, Liu T, A novel multi-link integrated factor algorithm considering node trust degree for blockchain-based communication, *KSII Trans Internet Inf Syst*, **11** (2017).

11 Gomez-Aravalli ADLR, Papadimitratos P, Blockchain-based public key infrastructure for inter-domain secure routing, *International Workshop on Open Problems in Network Security (iNetSec)*, May 2017, Rome, Italy. ffhal-01684192f, **5** (2017) 20–38.

12 Devi L, Shantharajah S P, Nirmal Kumar A, Authenticated and security maintance in wireless sensor network by filtering injected false data, *J Sci Ind Res*, **75(12)** (2016) 713–717.